SECURITY MANAGEMENT METHOD FOR NETWORK SYSTEM

Patent Number: JP10269184
Publication date: 1998-10-09
Inventor(s): SAITO YOKO
Applicant(s):: HITACHI LTD
Requested Patent: ☐ JP10269184
Application Number: JP19970076954 19970328
Priority Number(s):
IPC Classification: G06F15/00 ; G06F1/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a security management method for facilitating transition from a present user authentication system by a user ID and a password to a single sign-on by the utilization of a certificate.
SOLUTION: A job is requested by transmitting the information of the certificate from a client 8 to a job server 6 and the confirmation of the certificate is requested by transmitting the information of the certificate from the job server 6 to an integrated authentication server 2. The integrated authentication server 2 confirms the certificate, then obtains the security information of a user from a server 3 and checks the right to access the job server 6 of the user. At the time of appropriate access, the user ID, the password and access-to- data control information are sent to the job server 6. The job server 6 performs the authentication processing on the user and manages the access right to data thereafter. It is similar for a DB(data base) server 5 as well.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－269184

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ
1/00	３７０	1/00	３７０Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－76954

(22)出願日　平成９年(1997)３月28日

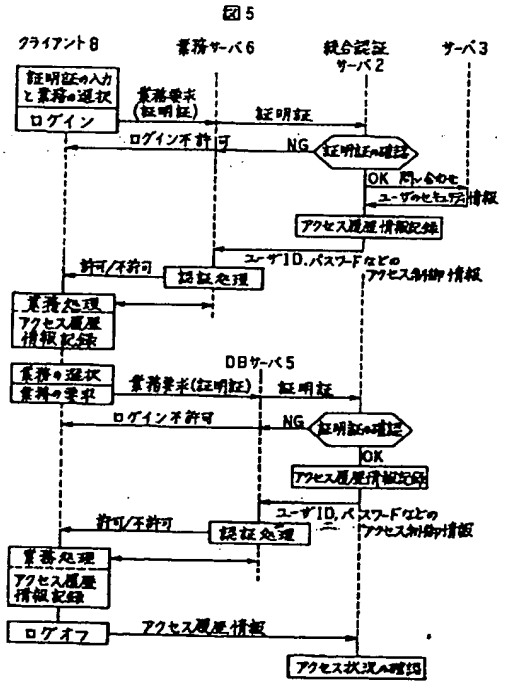
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　齋藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(74)代理人　弁理士　高橋　明夫

(54)【発明の名称】　ネットワークシステムのセキュリティ管理方法

(57)【要約】

【課題】　現行のユーザＩＤとパスワードによるユーザ認証方式から証明証の利用によるシングルサインオンへの移行を容易にするようなセキュリティ管理方法を提供する。

【解決手段】　クライアント８から業務サーバ６へ証明証の情報を送信して業務要求を行い、業務サーバ６から統合認証サーバ２へ証明証の情報を送信して証明証の確認要求を行う。統合認証サーバ２は、証明証の確認を行った後、サーバ３から当該ユーザのセキュリティ情報を取得してユーザの業務サーバ６をアクセスする権限をチェックする。正当なアクセスであれば、業務サーバ６へユーザＩＤ，パスワード，データへのアクセス制御情報を送る。業務サーバ６はユーザの認証処理を行い、以後データへのアクセス権限を管理する。ＤＢサーバ５についても同様である。



1

【特許請求の範囲】

【請求項１】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムのセキュリティ管理方法であって、

クライアントから業務サーバへ証明証の情報を送信して業務要求を行い、業務サーバから統合認証サーバへ証明証の情報を送信して証明証の確認要求を行い、統合認証サーバによって証明証の確認とユーザの該業務サーバへのアクセス権限のチェックとを行い、正当であれば業務サーバへユーザＩＤとパスワードを送信し、該業務サーバによってユーザＩＤとパスワードによる認証を行うことを特徴とするセキュリティ管理方法。

【請求項２】統合認証サーバによって証明証の確認を行う代わりに、業務サーバによって証明証の確認を行い、業務サーバから統合認証サーバへ証明証の情報を送信してユーザＩＤとパスワードの要求を行い、統合認証サーバによってユーザの該業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへユーザＩＤとパスワードを送信し、該業務サーバによってユーザＩＤとパスワードによる認証を行うことを特徴とする請求項１記載のセキュリティ管理方法。

【請求項３】該クライアントによってシステムへのログインからログオフまでの間で該統合認証サーバ及び該業務サーバが実行する証明証の確認結果、該業務サーバへのアクセス権限のチェック結果、ユーザＩＤとパスワードの認証結果及び業務サーバが保持するデータへのアクセス権限のチェック結果を含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、該統合認証サーバによって証明証の確認結果及び該業務サーバへのアクセス権限のチェックを含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、該クライアントが記録するアクセス履歴情報と該統合認証サーバが記録するアクセス履歴情報とを突き合わせることによってユーザのアクセス状況をチェックすることを特徴とする請求項１記載のセキュリティ管理方法。

【請求項４】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムにおいて該統合認証サーバによって読み取り可能な記憶媒体上に実体化されたコンピュータプログラムであって、該プログラムは以下のステップを含む：（ａ）クライアントから業務サーバを経由して送信された証明証の情報を受信し、（ｂ）該証明証が正当であることを確認し、（ｃ）該証明証のユーザが該業務サーバにアクセスする権限があるか否かをチェックし、（ｄ）（ｂ）及び（ｃ）のチェック結果が妥当であれば該業務サーバによって該ユーザの認証を行うように該ユーザのユーザＩＤとパスワードを該業務サーバへ送信する。

【請求項５】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムにおいて該統合認証サーバによって読み取り可能な記憶媒体上に実体化されたコンピュータプログラムであって、該プログラムは以下のステップを含む：（ａ）クライアントから第１の業務サーバを経由して送信されたユーザＩＤとパスワードを受信し、（ｂ）該ユーザＩＤのユーザが第１の業務サーバにアクセスする権限があるか否かをチェックし、（ｃ）（ｂ）のチェック結果が妥当であれば該ユーザの一時的な証明証を作成し、（ｄ）第１の業務サーバを経由してクライアントへ該証明証を送信し、（ｅ）クライアントから第２の業務サーバを経由して送信された該証明証の情報を受信し、（ｆ）該証明証が正当であることを確認し、（ｇ）該証明証のユーザが第２の業務サーバにアクセスする権限があるか否かをチェックし、（ｈ）（ｆ）及び（ｇ）のチェック結果が妥当であれば第２の業務サーバによって該ユーザの認証を行うように該ユーザのユーザＩＤとパスワードを第２の業務サーバへ送信する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアントとサーバを有するネットワークシステムのセキュリティ管理方法に係わり、特にユーザの一元管理を行い、ユーザに対して証明証を利用するシングルサインオン機能を提供するネットワークシステムのセキュリティ管理方法に関する。

【０００２】

【従来の技術】インターネットの普及に伴ってセキュリティ管理をめぐる市場動向はめざましく変化している。特にインターネットのような広域ネットワークシステムと企業内ネットワークシステムとを結合するとき、これら両ネットワークを統合するようなユーザ認証機能及びネットワークシステム内の資源へのアクセスを制御する機能が求められている。すなわち広域ネットワークシステムと企業内ネットワークシステムの両者に亘ったユーザの一元管理とネットワーク資源の集中管理が望まれる。

【０００３】広域ネットワークシステムを利用するユーザを一元管理する方法として、例えば特開平６－２２３０４１号公報に記載されるように利用者の個人情報と利用環境情報を秘密鍵によって暗号化した情報を証明書として発行し、利用者がこの証明書を利用してシステムにログインする方法がある。また分散システムを考慮するセキュリティ管理方法として、例えば特開平８－１０６４３７号公報に記載されるように、ユーザがそのホームドメインでないドメインへアクセスするときその資格認定を証明するログオン証明書を利用する方法がある。また特開平７－１４１２９６号公報は、ネットワークドメインをまたがってセキュリティを管理するＴＴＰ（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）を設け、ネットワーク全体のセキュリティポリシィの設定、変更及びセキュリティポリシィに基づくアクセス制御を行うシステ

ムを開示する。

【０００４】

【発明が解決しようとする課題】以上述べたように証明証を利用してユーザ認証及びアクセス制御を行う方式は、今後の広域ネットワークシステムのセキュリティ管理方式の１つとして普及するものとみられる。しかし現実のネットワークシステムを考慮すると、現在の企業ネットワークシステムは、外部の証明証発行機関が発行する証明証を利用する方式にすぐに移行したり、ＴＴＰによるセキュリティ管理に移行するのが困難であると考えられる。すなわち現行のユーザＩＤとパスワードによるユーザ認証方式を残しながら証明証の利用によるシングルサインオン方式を導入していく方法が現実的と考えられる。

【０００５】本発明の目的は、現行のユーザＩＤとパスワードによるユーザ認証方式から証明証の利用によるシングルサインオンへの移行を容易にするようなセキュリティ管理方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明は、ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムのセキュリティ管理方法であって、クライアントから業務サーバへ証明証の情報を送信して業務要求を行い、業務サーバから統合認証サーバへ証明証の情報を送信して証明証の確認要求を行い、統合認証サーバによって証明証の確認とユーザの業務サーバへのアクセス権限のチェックとを行い、正当であれば業務サーバへユーザＩＤとパスワードを送信し、業務サーバによってユーザＩＤとパスワードによる認証を行うセキュリティ管理方法を特徴とする。

【０００７】なお統合認証サーバによって証明証の確認を行う代わりに、業務サーバによって証明証の確認を行い、業務サーバから統合認証サーバへ証明証の情報を送信してユーザＩＤとパスワードの要求を行い、統合認証サーバによってユーザの業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへユーザＩＤとパスワードを送信し、業務サーバによってユーザＩＤとパスワードによる認証を行うようにしてもよい。

【０００８】また本発明は、クライアントから業務サーバへユーザＩＤとパスワードを送信して業務要求を行い、業務サーバから統合認証サーバへ当該ユーザＩＤとパスワードを送信し、統合認証サーバによってユーザの業務サーバへのアクセス権限のチェックを行い、正当であれば一時的な証明証を作成して業務サーバを経由してクライアントへ送信するセキュリティ管理方法を特徴とする。

【０００９】また本発明は、クライアントによってシステムへのログインからログオフまでの間で統合認証サーバ及び業務サーバが実行する証明証の確認結果、業務サーバへのアクセス権限のチェック結果、ユーザＩＤとパスワードの認証結果及び業務サーバが保持するデータへのアクセス権限のチェック結果を含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、統合認証サーバによって証明証の確認結果及び業務サーバへのアクセス権限のチェックを含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、クライアントが記録するアクセス履歴情報と統合認証サーバが記録するアクセス履歴情報とを突き合わせることによってユーザのアクセス状況をチェックするセキュリティ管理方法を特徴とする。

【００１０】さらに統合認証サーバによって読み取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して上記方法の統合認証サーバ側の処理を行うことができる。

【００１１】

【発明の実施の形態】以下本発明の一実施形態について図面を用いて説明する。

【００１２】図１は、本実施形態のネットワークシステムの構成図である。インターネットのような広域ネットワーク１０には、企業ネットワークシステム１と他企業ネットワークシステム９が接続される。企業ネットワークシステム１には、クライアント８のほかに、統合認証サーバ２、セキュリティ情報を管理するサーバ３、データベース（ＤＢ）サーバ５、業務サーバ６、グループウェアサーバ４、鍵管理サーバ１７、証明証発行サーバ１８等のサーバが接続される。ＤＢサーバ５及び業務サーバ６は、クライアント８からアクセスされ、業務処理のために利用されるサーバである。グループウェアサーバ４は、クライアント８へ最初の業務メニュー画面を送ったり、クライアント８へ電子メールを送ったり、ユーザのスケジュールを管理するサーバである。サーバ３はＤＢサーバ５及び業務サーバ６へのアクセスを制御する情報とユーザＩＤとパスワードのような認証情報を含むユーザのアクセス制御情報とから成るセキュリティ情報を一元的に管理するサーバである。統合認証サーバ２は、クライアント８から送られる証明証を確認し、サーバ３からセキュリティ情報を取得してユーザのＤＢサーバ５及び業務サーバ６へのアクセス権限をチェックするサーバである。鍵管理サーバ１７は、企業ネットワークシステム１内での暗号化通信で使用するマスタ鍵を生成するサーバである。広域ネットワーク１０には外部証明証発行サーバ７が接続される。外部証明証発行サーバ７は、所定の手順に従って外部証明証を発行するサーバである。証明証発行サーバ１８は、統合認証サーバ２からの要求によって外部証明証をもたないユーザに対して証明証を発行するサーバである。なおいわゆるディレクトリサーバと呼ばれるサーバがサーバ３の情報を有していてもよい。またクライアント８及び各種サーバは、パソコン、ワークステーション等を含む情報処理装置である。さらにクライアント８及び各種サーバによって各々読み

取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して以下に詳述するクライアント８及び各種サーバの処理を行うことができる。

【００１３】クライアント８又は他企業ネットワークシステム９に接続されるクライアント２０からユーザの証明証の情報を入力して例えばＤＢサーバ５にログインすると、ＤＢサーバ５又は統合認証サーバ２が証明証の確認を行い、統合認証サーバ２がサーバ３からセキュリティ情報を取得してＤＢサーバ５へのアクセス権限をチェックする。アクセス権限があれば、ＤＢサーバ５へユーザＩＤ，パスワードなどの認証情報を送り、ＤＢサーバ５がユーザの認証処理を行う。ＤＢサーバ５を利用する業務処理が終了し、次に業務サーバ６にログインするとき、クライアント８はすでに入力済みの証明証を業務サーバ６に送信し、上記の手続きを行うことによってシングルサインオンが実現する。証明証をもたないユーザに対しては、ユーザＩＤとパスワード入力によるログインによって証明証を発行し、以後クライアント８は、別の業務サーバに移るごとにこの証明証を業務サーバへ送信し、シングルサインオンが可能である。

【００１４】図２は、セキュリティ情報を管理するサーバ３がセキュリティ情報を一元管理する方式を説明する図である。サーバ３を導入する前に各サーバごとに管理していたユーザ及び資源（文書、データベース、端末装置、アプリケーションプログラム等）に関するセキュリティ情報をＬＤＡＰ情報変換プログラムによってＬＤＡＰ形式に変換し、サーバ３へ送ってサーバ３で一元管理する。ここにＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄａｔａ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）は、ＩＥＴＦ標準のディレクトリアクセスプロトコルである。

【００１５】図３は、ＬＤＡＰ形式の情報の例として、文書の定義と業務サーバのアクセス制御情報の形式を示す図である。文書の定義は、文書識別情報と文書のアクセス制御情報から構成される。文書識別情報は、文書の識別子、この文書を管理するサーバの識別子と組織名称並びに文書の情報（文書のタイトル、文書の更新日付、文書管理者、文書検索のためのキーワード、主題、アブストラクト、作者名）から構成される。一方文書のアクセス制御情報は、アクセス制御情報、最終修正情報、セキュリティポリシィ等を含む。アクセス制御情報は文書内の特定ページのアクセス制御情報のように文書の一部についてアクセス制御をする情報である。最終修正情報はアクセス制御情報の更新日付である。セキュリティポリシィはその文書にアクセスを許可するユーザのアクセスレベルを設定するものである。例えばポリシィ番号が１から３までのユーザに該当文書をアクセス許可するという運用が可能である。文書の定義は、業務サーバ６が管理する情報である。

【００１６】業務サーバのＡＣＬ（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｌｉｓｔ：アクセス制御リスト）情報として、業務サーバ６をアクセスするときのアクセス制御情報、アクセス制御情報の管理元サーバの識別子、ドメインセキュリティの定義の更新日付、セキュリティポリシィとしてデフォルトセキュリティポリシィ及び認可セキュリティポリシィ、及び経由するＤＳＡ（Ｄｏｍａｉｎ　ＳｅｃｕｒｉｔｙＡｕｔｈｏｒｉｔｙ）を定義している。認可セキュリティポリシィは、例えばポリシィ番号が１から５までのユーザに業務サーバ６のアクセスを許可するという運用が可能である。経由するＤＳＡによれば、ユーザの認証は必ず統合認証サーバ２を経由して行うよう定義する。業務サーバのアクセス制御情報は、サーバ３が保持し、統合認証サーバ２が管理する情報である。

【００１７】なお上記のアクセス制御情報のほかに、業務サーバ６にアクセスし、特定の文書にアクセスするユーザについてもアクセス制御情報を設定する必要がある。ユーザのアクセス制御情報は、ユーザの証明証の情報、ユーザＩＤとパスワードのような認証情報、ユーザの属する部門と職制情報、ユーザのアクセスレベル（ポリシィ番号）等を設定する。アクセスレベルの設定によって、例えばポリシィ番号が４のユーザは業務サーバ６にはアクセス可能であるが、ＸＸＸＸという文書へのアクセスを許可しないという運用が可能である。またある職制以上のユーザに対して特定の文書のアクセスを許可するような運用も可能である。

【００１８】図４は、統合認証サーバ２がサーバ３からユーザのセキュリティ情報を取得する手順を示す図である。セキュリティ情報を取得する手順には、ＬＤＡＰプロトコルが使用される。統合認証サーバ２は、まずｌｄａｐ＿ｏｐｅｎによってサーバ３とＬＤＡＰコネクションを確立し、ｌｄａｐ＿ｓｉｍｐｌｅ＿ｂｉｎｄ＿ｓによって統合認証サーバ２とサーバ３との間の相互認証を行った後、ｌｄａｐ＿ｓｅａｒｃｈ＿ｓによって統合認証サーバ２からユーザの証明証番号、ユーザＩＤなどを送信すると、サーバ３から統合認証サーバ２へそのユーザのセキュリティ情報を送信する。

【００１９】図５は、クライアント８のユーザが企業ネットワークシステム１にログインしてからログオフするまでの処理の手順を示す図である。ここではユーザが証明証（外部証明証を含む）を用いてログインする場合の手順について説明する。クライアント８は、業務メニューをクライアント８の表示装置に表示する。ユーザが業務サーバ６を選択し、証明証の情報をＩＣカード等の記憶媒体から入力すると、クライアント８は、証明証の情報をユーザの秘密鍵で暗号化して記憶装置に格納した後、業務要求とユーザの秘密鍵で暗号化された証明証の内容を業務サーバ６へ送信する。業務サーバ６は、統合認証サーバ２へ証明証の情報を送りその内容の確認要求を行う。統合認証サーバ２は、暗号化された証明証をユーザの公開鍵で復号化した後、その証明証の確認を行

う。証明証のデータ構成はＸ．５０９で規定されており、その内容は所有者氏名、発行元、発行元の署名、有効期限等の情報から成る。発行元の署名は発行者の秘密鍵で暗号化されているので、まずこの署名を発行元の公開鍵で復号して原本と比較し、証明証が正当なものであることを確認する。次に有効期限等内容の確認を行う。証明証が不適当なものであれば（ＮＧ）、業務サーバ６を経由してクライアント８へログイン不許可のメッセージを送信する。証明証が適当なものであれば（ＯＫ）、サーバ３へ問い合わせを行ってユーザのセキュリティ情報を取得する。その手順については上記した通りである。ユーザのセキュリティ情報は、業務サーバ６のアクセス制御情報とユーザのアクセス制御情報から構成される。統合認証サーバ２は、ユーザのアクセスレベルと業務サーバ６のアクセスレベルとを比較し、業務サーバ６のアクセスを許可できるならば、当該ユーザのアクセスを許可する旨のアクセス履歴情報を記憶装置に記録し、業務サーバ６へ暗号化したユーザＩＤ、パスワード、アクセスレベル、職制情報などユーザのアクセス制御情報を送信する。なお業務サーバ６がユーザＩＤに対応してアクセスレベル、職制情報などユーザのアクセス制御情報を保有している場合には、ユーザＩＤとパスワード以外のアクセス制御情報の送信は不要である。業務サーバ６は、受信したアクセス制御情報を復号し、まずユーザＩＤとパスワードが登録されているものに一致するか否か認証処理を行う。一致しなければ業務サーバ６へのアクセスを許可しない。一致すればクライアント８へ許可のメッセージを送信する。以後クライアント８から文書のアクセス要求があるごとに文書のアクセス制御情報とユーザのアクセスレベル、職制情報とから文書のアクセスを許可するか否かを決定する。クライアント８からは業務サーバ６が保有する文書にアクセス要求をして業務処理を行う。クライアント８は、業務処理の間、アクセスする文書についてアクセス履歴情報を記憶装置に記録する。

【００２０】このようにして業務サーバ６に係わる業務処理を終了した後、再び業務メニューをクライアント８の表示装置に表示する。ユーザが次にＤＢサーバ５を選択したとすれば、クライアント８は記憶していた当該ユーザの証明証を取り出して業務要求とともにＤＢサーバ５へ送信する。従ってユーザは再度証明証の情報を入力する必要がない。ＤＢサーバ５は、統合認証サーバ２へ証明証の情報を送りその内容の確認要求を行う。以後上記と同様に統合認証サーバ２は、暗号化された証明証をユーザの公開鍵で復号化した後、証明証の確認を行い、証明証の確認結果と当該ユーザのＤＢサーバ５へのアクセスを許可／不許可する旨のアクセス履歴情報を記録し、ＤＢサーバ５へアクセス制御情報を送信する。ＤＢサーバ５は、ユーザＩＤとパスワードによってユーザの認証処理を行う。ユーザのアクセスを許可したとき、以後受信したアクセス制御情報に基づいて指定されたデータベース、テーブル、テーブルの列などのアクセスを許可するか否かを決定する。クライアント８は、ＤＢサーバ５を利用して業務処理を行い、業務処理の間、アクセスするデータベースについてアクセス履歴情報を記録する。このようにして業務処理が終了し、ユーザがログオフを入力すると、クライアント８は記録したアクセス履歴情報を統合認証サーバ２へ送り、記憶装置上に保管していた証明証の情報を消去する。統合認証サーバ２は、受信したアクセス履歴情報と統合認証サーバ２が記録したアクセス履歴情報を比較して妥当なアクセスであるか否かチェックする。

【００２１】なお図５の処理手順において、最初に業務サーバ６にログインする代わりにグループウェアサーバ４にログインする場合も同様の処理手順になる。

【００２２】図６は、業務サーバ６及びＤＢサーバ５が証明証の内容を確認する機能をもつ場合の処理の手順を示す図である。図６の手順が図５の手順と異なる点は、統合認証サーバ２の代わりに業務サーバ６及びＤＢサーバ５がユーザの秘密鍵で暗号化された証明証をユーザの公開鍵で復号化した後、証明証を確認する点である。各業務サーバが証明証の内容を確認するためには、証明証の発行元の公開鍵を取得し、発行元の署名を確認する機能が必要である。

【００２３】図７は、証明証をもたないユーザが企業ネットワークシステム１にログインしてからログオフするまでの処理の手順を示す図である。ユーザが業務メニューの中から業務サーバ６を選択し、ユーザＩＤとパスワードを入力すると、クライアント８は、業務要求とユーザＩＤ，パスワードを業務サーバ６へ送信する。業務サーバ６は受け取ったユーザＩＤとパスワードが登録されているものに一致するか否か認証処理を行う。一致していなければ業務サーバ６へのアクセスを拒否する。一致しているとき業務サーバ６は、統合認証サーバ２へ受信したユーザＩＤとパスワードを送る。統合認証サーバ２は、サーバ３へユーザＩＤとパスワードを送って問い合わせを行い、ユーザのセキュリティ情報を取得する。次に統合認証サーバ２は、サーバ３から受け取ったセキュリティ情報に基づく上記のチェック処理によってユーザが業務サーバ６にアクセスする権限があるか否かチェックする。ユーザに権限がなければ（ＮＧ）、クライアント８へログイン不許可のメッセージを送信する。ユーザに権限があれば（ＯＫ）、証明証を発行する。この証明証は一時的に業務サーバ６へのアクセスを許可する目的で発行されるものなので、その有効期限は通常の証明証より短く（例えば当日限りなど）、業務サーバ６へのアクセス権限も制限される。次に統合認証サーバ２は、業務サーバ６へ証明証とアクセスレベル、職制情報などユーザのアクセス制御情報を送信する。業務サーバ６がアクセス制御情報を保有している場合には、アクセス制御

情報の送信は不要である。業務サーバ６は、受信した証明証をクライアント８へ送信する。クライアント８は、受信した証明証を記憶装置に格納したのち、業務サーバ６が保有する文書にアクセス要求をして業務処理を行う。業務サーバ６は、クライアント８から文書のアクセス要求があることに文書のアクセス制御情報とユーザのアクセスレベル、職制情報とから文書のアクセスを許可するか否かを決定する。クライアント８は、業務処理の間、アクセスする文書についてアクセス履歴情報を記録する。またクライアント８は、周期的に証明証の有効期限をチェックし、有効期限を過ぎる場合にはユーザに警告する。

【００２４】このようにして業務サーバ６に係わる業務処理を終了した後、ユーザがＤＢサーバ５を選択した場合、クライアント８は保管していた証明証を取り出して業務要求とともにＤＢサーバ５へ送信する。ＤＢサーバ５は、統合認証サーバ２へ証明証の情報を送り、その内容の確認要求を行う。統合認証サーバ２は、上記のように証明証の確認を行い、ＤＢサーバ５へユーザＩＤ，パスワードを含むアクセス制御情報を送信する。ＤＢサーバ５は、ユーザＩＤ，パスワードによる認証処理を行い、正当であればＤＢサーバ５へのアクセスを許可する。以後上記のようにクライアント８はＤＢサーバ５にデータベースのアクセス要求を送信し、ＤＢサーバ５はユーザのアクセス制御情報に基づいてデータベースのアクセスを許可するか否かを決定する。クライアント８はＤＢサーバ５を利用して業務処理を行い、業務処理の間、アクセスするデータベースについてアクセス履歴情報を記録する。このようにして業務処理を終了し、ユーザがログオフを入力すると、クライアント８は記録したアクセス履歴情報を統合認証サーバ２へ送り、保管していた証明証の情報を消去する。統合認証サーバ２は、受信したアクセス履歴情報と統合認証サーバ２が記録したアクセス履歴情報とを比較して妥当なアクセスであるか否かチェックする。ログオフ手続きの一環としてユーザから証明証の発行要求があれば、クライアント８はこの要求を統合認証サーバ２へ送信する。統合認証サーバ２は、当該ユーザのセキュリティ情報とアクセス状況に問題があるか否かチェックする。すなわち統合認証サーバ２がユーザの権限確認の後のアクセス履歴情報にログイン許可の記録がなければ、当然問題ありとなる。またその後のＤＢサーバ５のアクセス許可の記録がないにもかかわらずクライアント８側のアクセス履歴情報にＤＢサーバ５にアクセスした記録がある場合にも問題ありとなる。またクライアント８が業務サーバ６及びＤＢサーバ５の文書やデータベースにアクセスするとき不許可のケースがクライアント８側のアクセス履歴情報に記録されていれば問題が生じている。問題があるとき（ＹＥＳ）、統合認証サーバ２は、クライアント８へ証明証の発行を許可しない旨のメッセージを送信する。問題がなければ（ＮＯ）、統合認証サーバ２は、証明証発行サーバ１８へ証明証の発行要求を送信し、証明証発行サーバ１８が証明証を発行して統合認証サーバ２へ送信し、統合認証サーバ２がこの証明証をクライアント８へ送信する。クライアント８は受信した証明証をＩＣカード、フロッピィディスク等の外部記録媒体に出力する。この後ユーザは、図５に示す証明証を用いるログイン手続きを行うことができる。このように本実施形態によれば、証明証をもたないユーザがログインする場合も１回のログインによるシングルサインオンを実現できる。なお統合認証サーバ２、業務サーバ６及びＤＢサーバ５は、図５に示す処理手順と図７に示す処理手順の両方を併行してサポートするのが望ましい。

【００２５】図８は、統合認証サーバ２がユーザのアクセス状況を監視してセキュリティ侵害を検出する処理の手順を示す図である。クライアント８と統合認証サーバ２が連携することによってユーザのアクセス状況をチェックし、システムへのセキュリティ侵害を検出することが可能である。図８の例ではクライアント８が業務サーバ６にアクセスして業務処理を行っているとき、ある文書についてアクセス要求をすると、業務サーバ６がユーザのアクセス制御情報と文書のアクセス制御情報とからアクセスチェックを行い、その結果不当なアクセス要求であればクライアント８へアクセス不許可のメッセージを返す状態を示している。クライアント８は、このアクセス不許可をアクセス履歴情報に記録する。クライアント８がログオフを指示すると、クライアント８で記録された当該ユーザについてのアクセス履歴情報を統合認証サーバ２へ送信する。統合認証サーバ２は、統合認証サーバ２が採取したアクセス履歴情報、クライアント８が採取したアクセス履歴情報及び両者の突き合わせからユーザのアクセス状況が正当か否かを判定する。もしユーザが不当なアクセス又は不適切なアクセスをしていると判定すれば、統合認証サーバ２は当該ユーザのアクセス制御情報を削除する処理を行う。

【００２６】ユーザの不当なアクセス又は不適切なアクセスとして例えば次のようなケースがある。

（ａ）統合認証サーバ２にログイン許可の記録がない。すなわち証明証の確認結果が不許可である。

（ｂ）統合認証サーバ２が行うユーザの権限確認チェックの結果、業務サーバへのアクセスを不許可にしているにもかかわらずクライアント８がその業務サーバにアクセスしている。

（ｃ）業務サーバ又はＤＢサーバが行う認証処理の結果が不許可である。

（ｄ）クライアント８が証明証の有効期限の期限切れを検出している。

（ｅ）クライアント８が許可されない文書やデータベースへのアクセスを試行している。

（ｆ）クライアント８が証明証を入力した時刻、ログイ

ン指令をした時刻、統合認証サーバ２が証明証を確認した時刻、業務サーバ６がユーザの認証を行って業務サーバ６へのアクセスを許可した時刻などアクセス履歴情報に記録されたセキュリティ関係の処理時刻が正しい時系列のシーケンスになっていない。

【００２７】本実施形態によれば、統合認証サーバ２及びサーバ３がユーザのアクセス制御情報と業務サーバのアクセス制御情報とから成るセキュリティ情報を一元管理するため、セキュリティ情報の登録と更新を集中的に行うことができ、従来のように各業務サーバがセキュリティ情報を個別に管理する必要がない。

【００２８】図９は、セキュリティ情報の登録、照会及び更新の手順を示す図である。図９（ａ）は、セキュリティ情報の登録フェーズの処理手順を示す図である。各サーバからサーバ３へセキュリティ情報の登録を要求すると、サーバ３は要求されたセキュリティ情報を記憶装置に登録する。このとき上述したようにＬＤＡＰ情報変換プログラムを利用して既存のセキュリティ情報をＬＤＡＰ形式に変換することができる。図９（ｂ）は、セキュリティ情報の照会の手順を示す図である。各サーバから統合認証サーバ２へセキュリティ情報を問い合わせる。統合認証サーバ２は、指定されたユーザに関するセキュリティ情報をすでに取り込んでいれば（ＹＥＳ）、そのセキュリティ情報を回答する。取り込んでなければ（ＮＯ）、サーバ３に問い合わせてセキュリティ情報を取得してから要求元のサーバに回答する。例えば図６に示す業務サーバ６及びＤＢサーバ５が証明証情報を統合認証サーバ２へ送信してセキュリティ情報を照会する場合がこれに相当する。また図７に示す業務サーバ６がユーザＩＤとパスワードを統合認証サーバ２へ送信してユーザの権限確認を依頼し、証明証の発行を依頼し、ユーザのアクセス制御情報を受ける場合もこれに相当する。図９（ｃ）は、セキュリティ情報の更新の例を示す図である。統合認証サーバ２がユーザによるセキュリティ侵害を検出したとき、各サーバへユーザの削除を通知する。またサーバ３へ当該ユーザについてアクセス制御情報の削除を要求する。

【００２９】なお統合認証サーバ２とサーバ３を分離せずに同一のサーバにしても本発明を実現できる。また統合認証サーバ２、サーバ３、鍵管理サーバ１７及び証明証発行サーバ１８を同一のサーバで実現することも可能である。

【００３０】最後にクライアント８、サーバ５，６及び統合認証サーバ２との間の暗号化通信について説明する。従来のユーザ情報、特にパスワード情報が通信回線上で盗聴されると、盗んだ情報を基にして他人に成りすましたりするセキュリティ上の脅威があった。本発明は、本来公開されて良い証明証の情報を用いてユーザを確認するため、証明証の情報に加えてユーザの秘密鍵の情報が盗まれれば悪意のある第三者が他人に成りすますことも有り得る。従ってクライアント８、サーバ５，６及び統合認証サーバ２との間の通信は、相互に通信相手の認証をした後に、暗号化通信により行われる必要がある。特に各サーバと統合認証サーバ２との間ではユーザに関するセキュリティ情報が送受信されるために、当事者だけが見られるように情報を保護する必要がある。セキュリティ情報を保護するための通信手段として、例えばＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）が知られている。

【００３１】暗号化通信を行うためには、暗号鍵の生成、配送及び回復のような鍵管理の問題がある。どのような暗号化手段を用いるかによって管理方法や実現方法が異なる。以下にＭｕｌｔｉ２と呼ばれるグループ鍵暗号方式による暗号化技術について説明する。

【００３２】図１０は、グループ鍵によるデータの暗号化処理の手順を説明する図である。鍵管理サーバ１７は、クライアント、及びサーバのマスタ鍵を作成し配布する。そしてこのマスタ鍵からメッセージを暗号化するために暗号鍵を生成するが、当メッセージを読ませたい相手（複数の指定が可能）を宛て先リストに登録し、マスタ鍵と宛て先リストから動的にグループ鍵を作成し、このグループ鍵によってメッセージを暗号化する。図１０の例では、クライアント８は、業務サーバ６にメッセージＡを送信する際に宛て先リストＡにクライアント８、業務サーバ６及び統合認証サーバ２を指定する。そして業務サーバ６に対してはグループ鍵Ａを送信せず、メッセージＡを暗号化したものと宛て先リストＡだけを送る。業務サーバ６は、クライアント８から受信したメッセージＡを復号化するために、メッセージＡとともに受信した宛て先リストＡとマスタ鍵から動的にグループ鍵Ａを作成する。業務サーバ６は、このようにして作成したグループ鍵Ａによりメッセージを復号化する。また業務サーバ６から統合認証サーバ２へメッセージＡを送信する場合にも、マスタ鍵と宛て先リストＡからグループ鍵Ａを作成し、送信したいメッセージＡをグループ鍵Ａで暗号化する。グループ鍵Ａは、宛て先リストＡに登録され、かつマスタ鍵を持つ相手でなければ動的に作成できないため、このように見せたい相手だけにメッセージＡを読ませることができる。

【００３３】次に統合認証サーバ２が業務サーバ６へメッセージＢを送信したい場合には、宛て先リストＢに業務サーバ６だけを設定し、マスタ鍵と宛て先リストＢから作成したグループ鍵Ｂによってメッセージを暗号化して送る。クライアント８がこの暗号化されたメッセージＢを解読しようとしても、クライアント８は宛て先リストＢに登録されていないために解読することができない。図１０の例では、クライアント８と各サーバ間のグループ鍵による暗号化通信を説明したが、ユーザごとにマスタ鍵を持たせることも可能である。この場合には、マスタ鍵をＩＣカード内に格納し、ＩＣカード中でグル

13

ープ鍵を生成することも可能である。

【００３４】

【発明の効果】以上述べたように本発明によれば、業務サーバやデータベースサーバが従来のユーザＩＤとパスワードに基づくユーザ認証とアクセス制御を保存しながらユーザに対して証明証利用によるシングルサインオンの機能を提供できる。また証明証をもたないユーザに対しても一時的な証明証の発行によるシングルサインオンを実現することができる。またクライアントと統合認証サーバが連携することによって、ユーザのアクセス状況を監視し、アクセス状況に問題があるユーザをシステムから除外することができる。

【図面の簡単な説明】

【図１】実施形態のネットワークシステムの構成図である。

【図２】実施形態のサーバ３がセキュリティ情報を一元管理する方式を説明する図である。

【図３】ＬＤＡＰ形式の情報の例を示す図である。

【図４】実施形態の統合認証サーバ２がサーバ３からユ＊

14

＊ーザのセキュリティ情報を取得する手順を示す図である。

【図５】実施形態の証明証を利用するシングルサインオンの処理手順を示す図である。

【図６】図５の処理手順で統合認証サーバ２の代わりにＤＢサーバ５／業務サーバ６が証明証を確認する処理手順を示す図である。

【図７】実施形態の証明証をもたないユーザによるシングルサインオンの処理手順を示す図である。

【図８】実施形態の統合認証サーバ２がユーザのアクセス状況を監視してセキュリティ侵害を検出する処理手順を示す図である。

【図９】実施形態のセキュリティ情報を管理する処理を説明する図である。

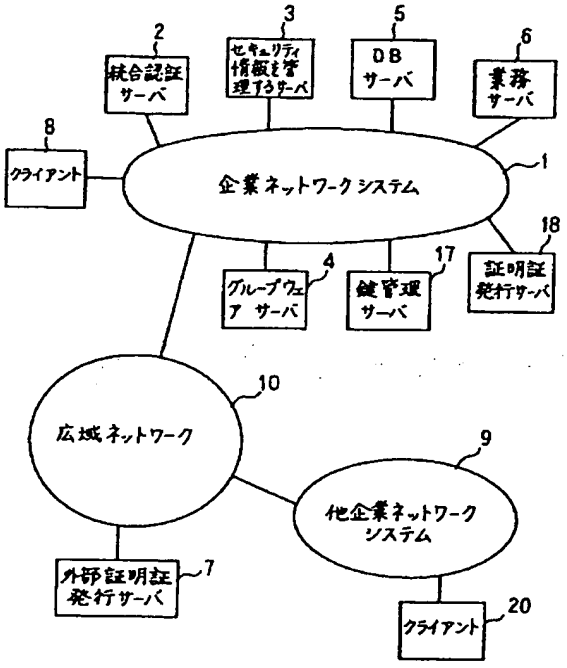
【図１０】グループ鍵によるデータの暗号化処理の手順を説明する図である。

【符号の説明】

２：統合認証サーバ、３：（セキュリティ情報を管理する）サーバ、１８：証明証発行サーバ

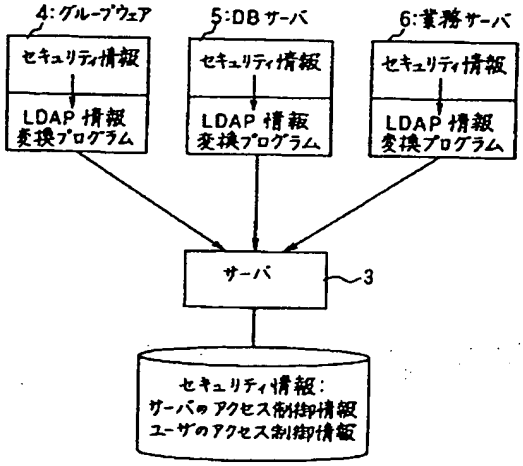
【図１】

図 1



【図２】

図 2



【図３】

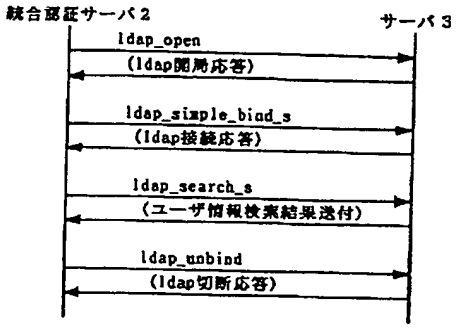
図３

文書ＸＸの定義：
文書識別情報：文書ＸＸ，業務サーバ６，組織名称，文書タイトル，更新日付，文書管理者，キーワード，主題，アブストラクト，作者名
文書ＸＸのアクセス制御情報：
アクセス制御情報，最終修正情報，セキュリティポリシィ

業務サーバ６のドメインセキュリティの定義：
ＡＣＬ情報：アクセス制御情報，管理元は統合認証サーバ２，ドメインセキュリティの定義更新日付，デフォルトセキュリティポリシィ，認可セキュリティポリシィ，経由するＤＳＡは統合認証サーバ２

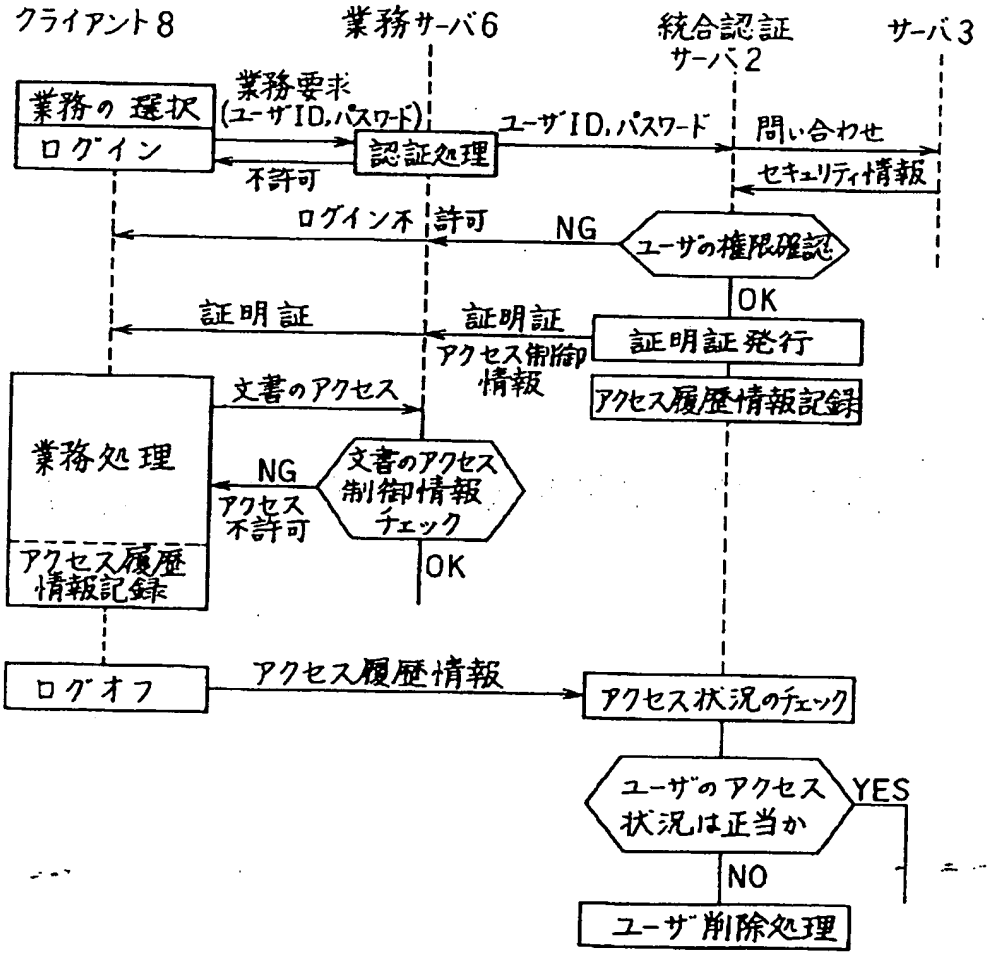
【図４】

図４



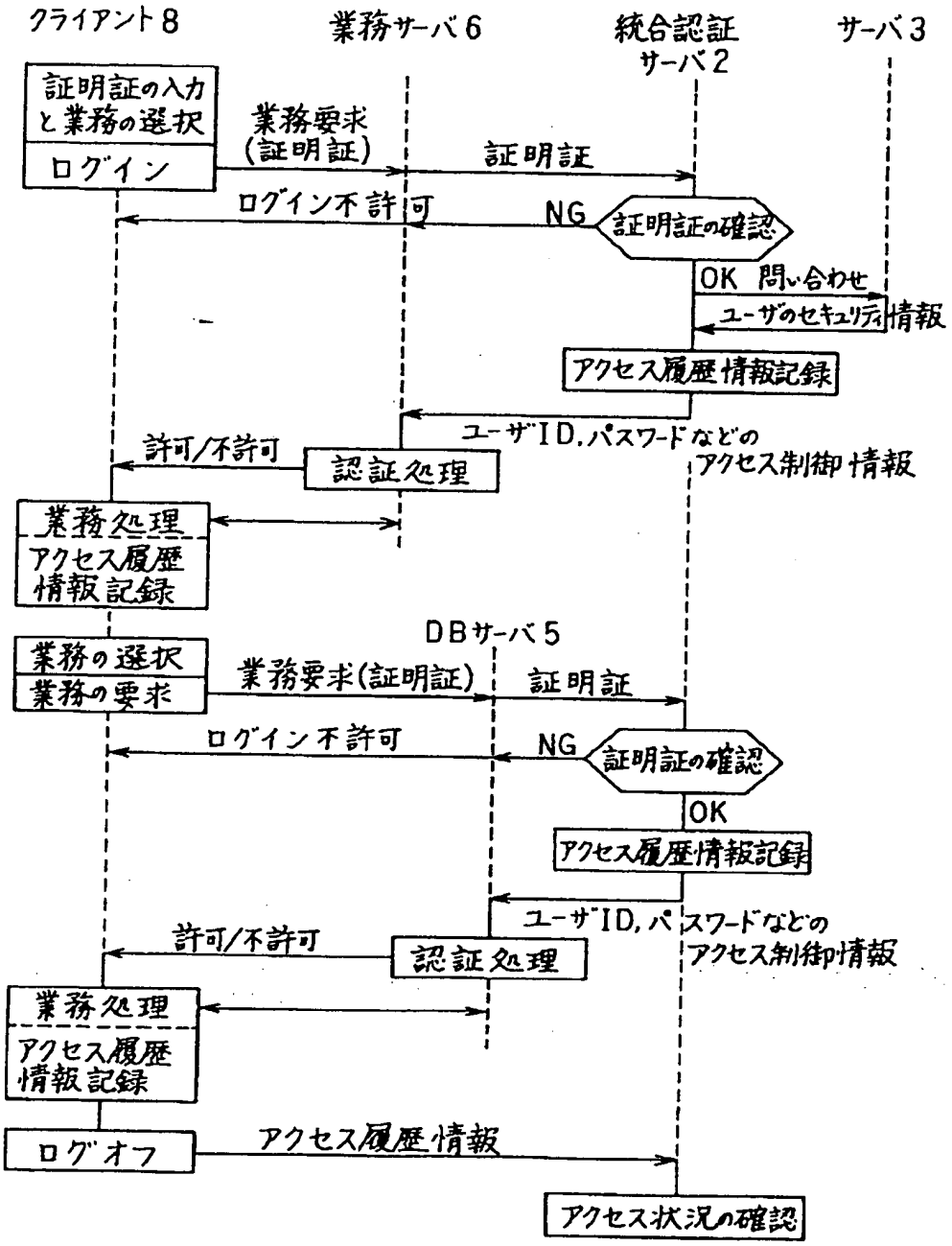
【図８】

図８



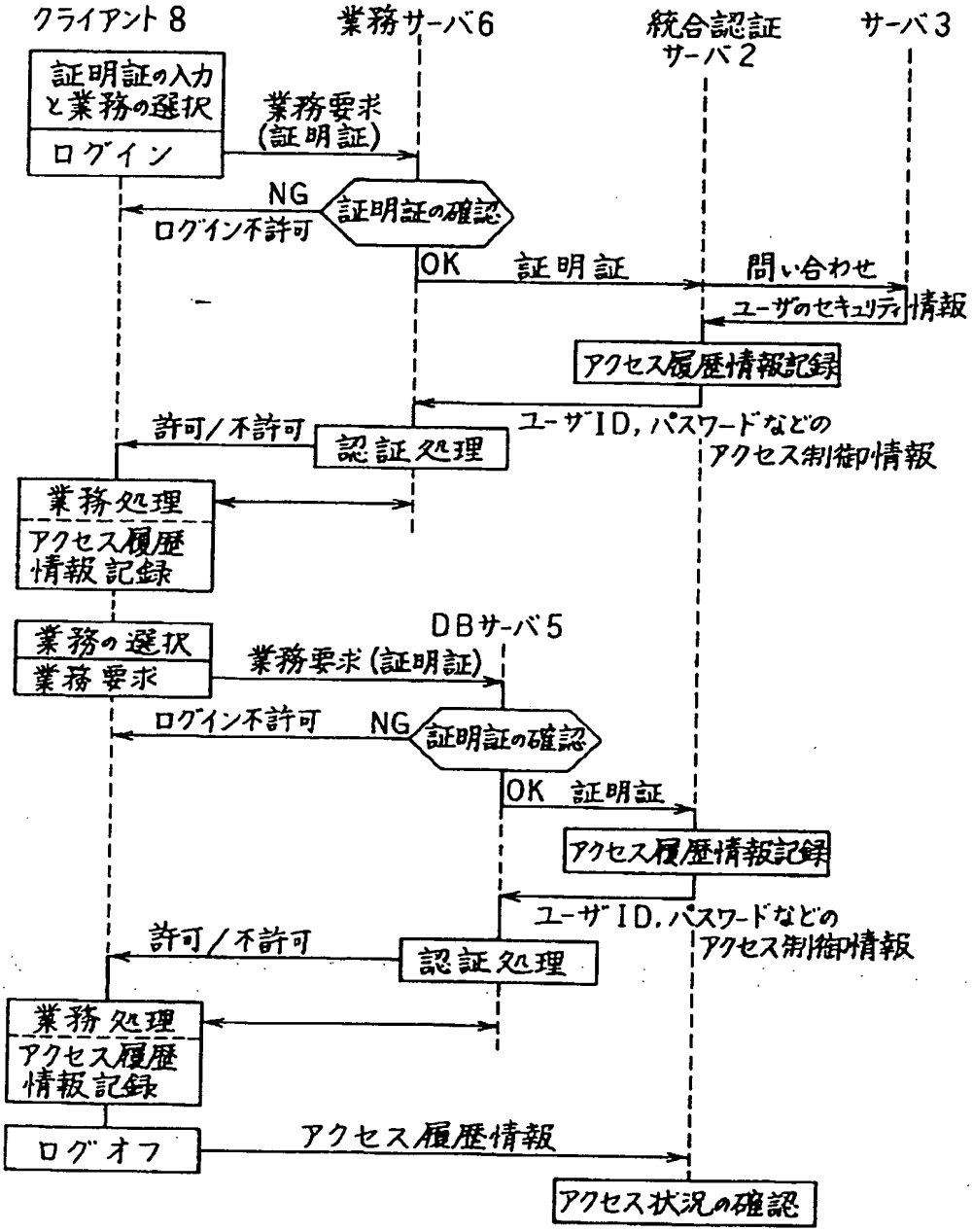
【図5】

図5


クライアント8
業務サーバ6
統合認証サーバ2
サーバ3
証明証の入力と業務の選択
ログイン
業務要求(証明証)
証明証
ログイン不許可
NG
証明証の確認
OK 問い合わせ
ユーザのセキュリティ情報
アクセス履歴情報記録
ユーザID,パスワードなどのアクセス制御情報
許可/不許可
認証処理
業務処理
アクセス履歴情報記録
DBサーバ5
業務の選択
業務の要求
業務要求(証明証)
証明証
ログイン不許可
NG
証明証の確認
OK
アクセス履歴情報記録
ユーザID,パスワードなどのアクセス制御情報
許可/不許可
認証処理
業務処理
アクセス履歴情報記録
ログオフ
アクセス履歴情報
アクセス状況の確認

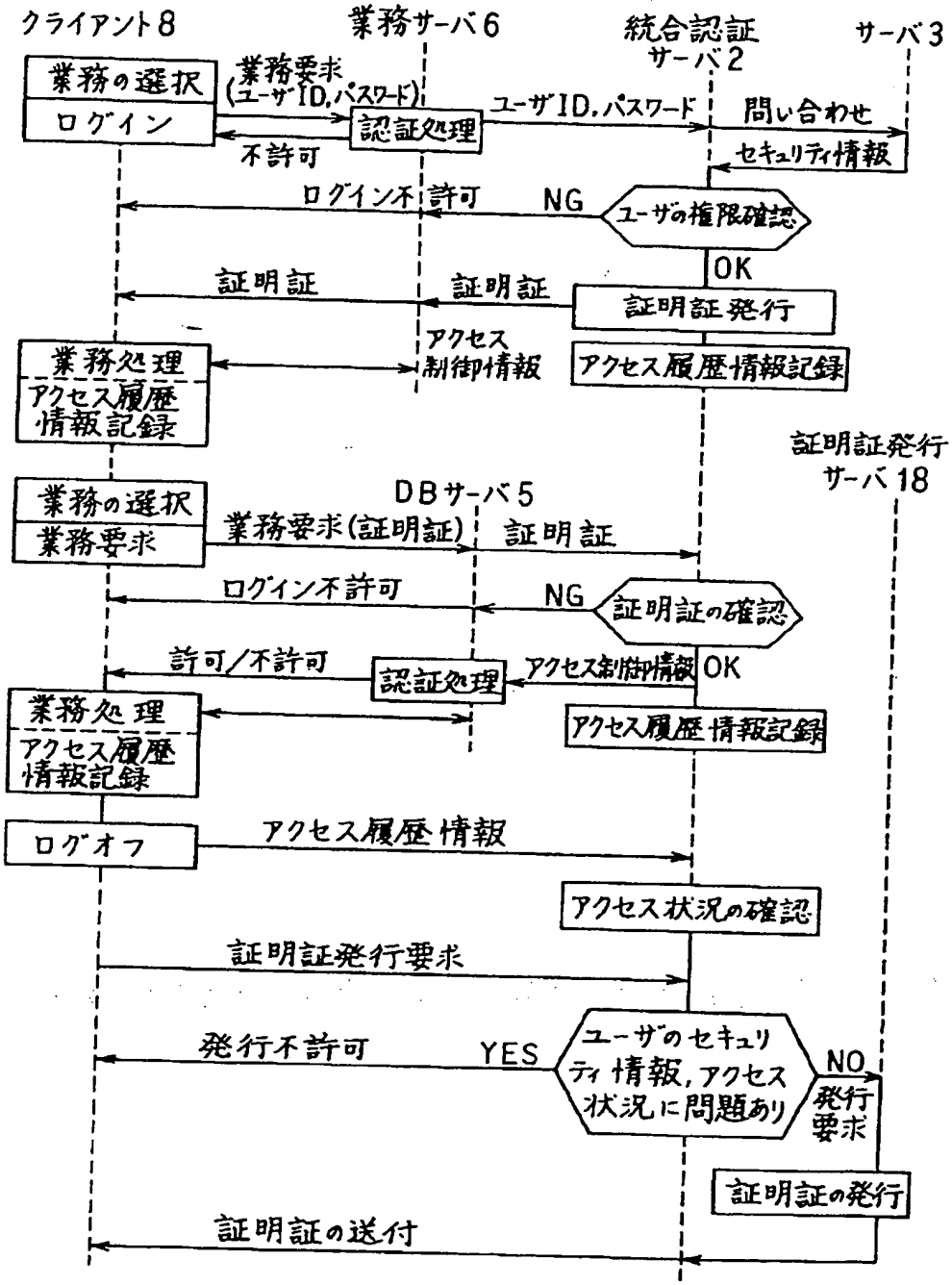
【図6】

図6


クライアント8
業務サーバ6
統合認証サーバ2
サーバ3
証明証の入力と業務の選択
ログイン
業務要求(証明証)
NG
証明証の確認
ログイン不許可
OK
証明証
問い合わせ
ユーザのセキュリティ情報
アクセス履歴情報記録
許可/不許可
認証処理
ユーザID,パスワードなどのアクセス制御情報
業務処理
アクセス履歴情報記録
DBサーバ5
業務の選択
業務要求
業務要求(証明証)
ログイン不許可
NG
証明証の確認
OK
証明証
アクセス履歴情報記録
ユーザID,パスワードなどのアクセス制御情報
許可/不許可
認証処理
業務処理
アクセス履歴情報記録
ログオフ
アクセス履歴情報
アクセス状況の確認

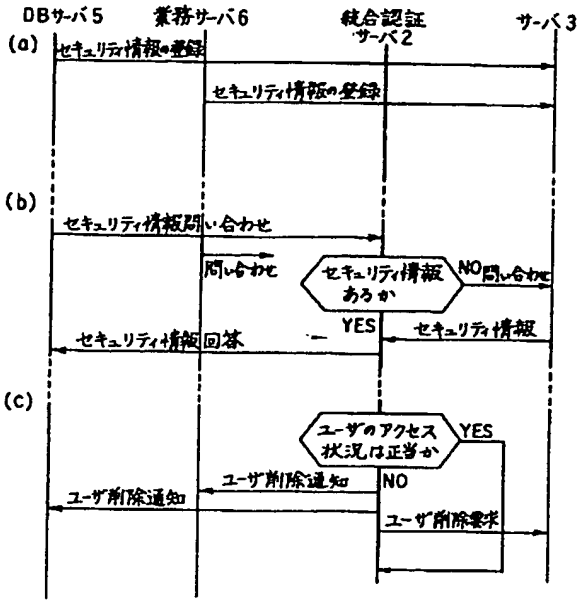
【図7】

図7


クライアント8
業務サーバ6
統合認証サーバ2
サーバ3
業務の選択
ログイン
業務要求(ユーザID,パスワード)
認証処理
ユーザID,パスワード
問い合わせ
セキュリティ情報
不許可
ログイン不許可
NG
ユーザの権限確認
OK
証明証
証明証
証明証発行
アクセス制御情報
アクセス履歴情報記録
業務処理
アクセス履歴情報記録
証明証発行サーバ18
DBサーバ5
業務の選択
業務要求
業務要求(証明証)
証明証
ログイン不許可
NG
証明証の確認
許可/不許可
認証処理
アクセス制御情報
OK
業務処理
アクセス履歴情報記録
アクセス履歴情報記録
ログオフ
アクセス履歴情報
アクセス状況の確認
証明証発行要求
発行不許可
YES
ユーザのセキュリティ情報,アクセス状況に問題あり
NO
発行要求
証明証の発行
証明証の送付

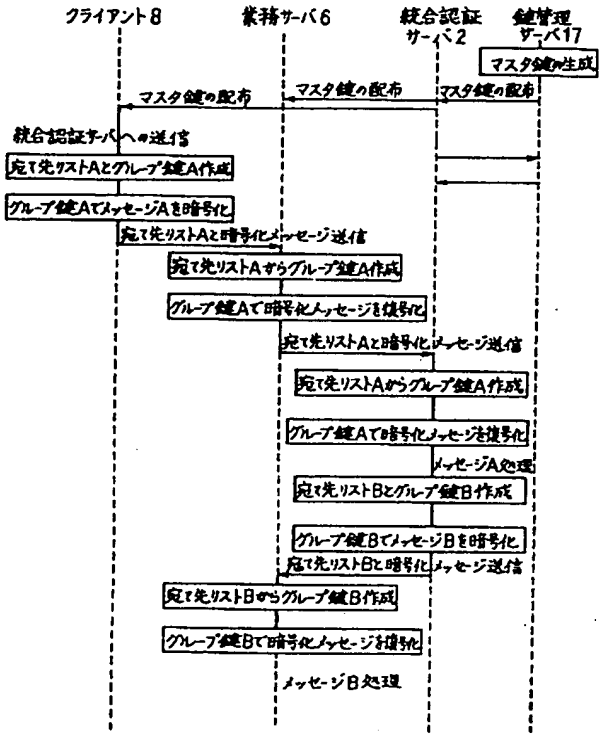
【図９】

図9


DBサーバ5
業務サーバ6
統合認証サーバ2
サーバ3
(a)
セキュリティ情報の登録
セキュリティ情報の登録
(b)
セキュリティ情報問い合わせ
問い合わせ
セキュリティ情報あるか
NO問い合わせ
YES
セキュリティ情報
セキュリティ情報回答
(c)
ユーザのアクセス状況は正当か
YES
NO
ユーザ削除通知
ユーザ削除通知
ユーザ削除要求

【図１０】

図10


クライアント8
業務サーバ6
統合認証サーバ2
鍵管理サーバ17
マスタ鍵の生成
マスタ鍵の配布
マスタ鍵の配布
マスタ鍵の配布
統合認証サーバへの送信
宛て先リストAとグループ鍵A作成
グループ鍵Aでメッセージを暗号化
宛て先リストAと暗号化メッセージ送信
宛て先リストAからグループ鍵A作成
グループ鍵Aで暗号化メッセージを復号化
宛て先リストAと暗号化メッセージ送信
宛て先リストAからグループ鍵A作成
グループ鍵Aで暗号化メッセージを復号化
メッセージA処理
宛て先リストBとグループ鍵B作成
グループ鍵Bでメッセージを暗号化
宛て先リストBと暗号化メッセージ送信
宛て先リストBからグループ鍵B作成
グループ鍵Bで暗号化メッセージを復号化
メッセージB処理